WebMemo
Published by The Heritage Foundation
No. 1735
December 12, 2007

Trojan Dragons: China's International Cyber Warriors

John J. Tkacik, Jr.

This week, *The New York Times* reported that in a series of "sophisticated attempts" against the U.S. nuclear weapons lab at Oak Ridge, Tennessee, Chinese hackers were able to "remove data."[1] The story illustrates an alarming fact: China's cyber spies are now a part of America's computer network, literally. It is time for U.S. authorities to be open with the American people about the escalating threat posed by China to America's science and technology secrets.

Continuous Attacks. U.S. Strategic Command Chief General James E. Cartwright told Congress in March 2007 that "America is under widespread attack in cyberspace." During fiscal year 2007, the Department of Homeland Security received 37,000 reports of attempted breaches on government and private systems, which included 12,986 direct assaults on federal agencies and more than 80,000 attempted attacks on Department of Defense computer network systems. Some of these attacks "reduced the U.S. military's operational capabilities."2 As for China's part in this trend, one American cyber security firm that focuses on "a centralised group of activity based from China" now says that "in the last three months, the attacks [from China] have almost tripled."[3]

A Global Threat. Officials in Europe have not hesitated to spotlight China's cyber warfare. Publicly, they have been more vocal and pointed about Chinese involvement than their American counterparts. Earlier this month, Jonathan Evans, the chief of Great Britain's domestic counterintelligence service, MI-5, sent a confidential letter to 300 accountants, legal firms, and chief executives and security chiefs at banks, warning them that they were under "electronic espionage attack" from "Chinese state organisations." Mr. Evans noted that a number of British companies—Rolls Royce is one example—had discovered that viruses of Chinese government origin were uploading vast quantities of industrial secrets to Internet servers in China.[4]

It was just the latest warning from European governments that China is the source of a breathtakingly broad campaign of cyber penetrations of European government and commercial information systems. In October, one of Germany's top internal security officers, Hans Elmar Remberg, told a Berlin conference on industrial espionage that his country was involved in "the Chinese cyber war"—and in case his audience was under the illusion that the aggressors were mere "hackers"—he averred, "In our view, state Chinese interests [*Chinesische Staatsinteressen*] stand behind these digital attacks." The German news magazine *Der Spiegel* termed the attackers as "The Yellow Spies."[5] The unfortunate use of racial language gave an opening to Chinese students in Germany to claim racism.[6] The charges of racism, of course, did not gainsay the facts presented by *Der Spiegel*.

This paper, in its entirety, can be found at:
www.heritage.org/Research/AsiaandthePacific/wm1735.cfm

Produced by the Asian Studies Center

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

In September, French Secretary General for National Defence Francis Delon said, "We have proof that there was involvement with China," but he demurred, "that is not to say the Chinese government."[7]

The German government has been particularly annoyed by the attacks. In August, German Chancellor Angela Merkel learned that three computer networks in her own office had been penetrated by Chinese intelligence services. A few days later, she confronted the visiting Chinese premier directly about the attacks and demanded that China play by the rules. Premier Wen Jiabao, straight-faced, expressed utter shock and promised that his government would get to the bottom of it. He then asked for detailed information from Germany's counterintelligence agencies to help China's security police find the culprit.[8]

By far, the target attacked most intensely by the Chinese is the U.S. military, closely followed by the State Department, the Commerce Department, and apparently the Department of Homeland Security. China also targets computer networks in sensitive U.S. sectors relating to commerce, academia, industry, finance, and energy. One U.S. cyber security expert told a group of federal managers that "the Chinese are in half of your agencies' systems" already.[9]

Lessons Not Learned. While the U.S. government may be reticent to reveal the vulnerabilities of its databases to Chinese penetration, the information available shows how widespread Chinese cyber attacks have become. Cyber warfare units in the Chinese People's Liberation Army (PLA) have already penetrated the Pentagon's unclassified Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and have designed software to disable it in time of conflict or confrontation.[10] Maj. Gen. William Lord, director of information, services, and integration in the Air Force's Office of Warfighting Integration admits that "China has downloaded 10 to 20 terabytes of data from the NIPRNet already," and added, "There is a nation-state threat by the Chinese."[11]

Richard Lawless, deputy undersecretary of defense for Asia-Pacific affairs, told a congressional

1. John Markoff, "China Link Suspected in Lab Hacking," *The New York Times*, December 9, 2007, p. A-03, at *www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html.*
2. Notes from a presentation by Dr. Andrew Palowitch entitled, "Cyber Warfare: Viable Component to the National Cyber Security Initiative?" at Georgetown University, November 27, 2007.
3. Stephen Fidler, "Steep Rise in Hacking Attacks from China," *The Financial Times*, December 5, 2007, at *www.ft.com/cms/s/0/c93e3ba2-a361-11dc-b229-0000779fd2ac.html.* Source cites Yuval Ben-Itzhak, chief technology officer for Finjan, a Web security group based in San Jose, California.
4. Rhys Blakely, Jonathan Richards, James Rossiter, and Richard Beeston, "MI5 Alert on China's Cyberspace Spy Threat," TimesOnline, December 1, 2007, at *http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece* (December 11, 2007).
5. The August 27, 2007, issue of *Der Spiegel* bore the cover title "Die Gelben Spione: Wie China deutsche Technologie ausspaht" (The Yellow Spies: How China Steals German Technology). The cover story was entitled "Chinesische Trojaner auf PCs im Kanzleramt" (Chinese Trojans in Chancellor Office PCs), *Der Spiegel*, posted August 25, 2007, at *www.spiegel.de/netzwelt/tech/0,1518,501954,00.html.*
6. "Zai De Huaren; Gao Mingjing Zui Hua" (Chinese in Germany; Spiegel Slanders Chinese), *Shijie Ribao*, December 7, 2007, at *www.worldjournal.com/wj-ch-news.php?nt_seq_id=1635448.*
7. (No author cited), "Now France Comes Under Attack from PRC Hackers," Agence France Presse, September 9, 2007, at *www.taipeitimes.com/News/front/archives/2007/09/09/2003377917.*
8. John Blau, "German Gov't PCs Hacked, China Offers to Investigate: China Offers to Help Track Down the Chinese Hackers Who Broke into German Computers," *PC World*, August 27, 2007, at *www.washingtonpost.com/wp-dyn/content/article/2007/08/27/AR2007082700595.html.*
9. Mark A Kellner, "China a 'Latent Threat, Potential Enemy': Expert," *DefenseNews Weekly*, December 4, 2006, at *www.defensenews.com/story.php?F=2389588&C=america.*
10. Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency."
11. (No author cited), "Pentagon warns of Internet incursion by Chinese cyber-terrorists," GCN, August 24, 2006.

panel on June 13, 2007, that the Chinese are "leveraging information technology expertise available in China's booming economy to make significant strides in cyber-warfare." He noted that the Chinese military's "determination to familiarize themselves and dominate to some degree the Internet capabilities—not only of China and that region of the world—provide them with a growing and very impressive capability that we are very mindful of and are spending a lot of time watching."[12]

The Chinese, he said,

> have developed a very sophisticated, broadly-based capability to...attack and degrade our computer systems and our Internet systems. Computer access, warfare and the...disruptive things that that allows you to do to an opponent are well appreciated by the Chinese and they spend a lot of time figuring out how to disrupt our networks—how to both penetrate networks, in terms of gleaning or gaining information that is protected, as well as computer network attack programs which would allow them to shut down critical systems at times of emergency. So first of all, the capability is there. They're growing it; they see it as a major component of their asymmetric warfare capability.[13]

PLA cyber warfare units have access to source codes for America's ubiquitous office software, giving them a skeleton key to every networked government, military, business, and private computer in America. General Cartwright has warned, "I think that we should start to consider that 'regret factors' associated with a cyber attack could, in fact, be in the magnitude of a weapon of mass destruction."[14]

What the U.S. Must Do . As the alarming state of cyber security becomes ever clearer, the Administration should build on the statements of General Lord and former Deputy Undersecretary Lawless. China's cyber warriors are the most acute threat not only to America's national security information infrastructure but to commercial, financial, and energy information networks as well. And via their computer network operations, China's clandestine intelligence collection is the top intelligence threat to America's science and technology secrets. If the Administration believes otherwise, it ought to explain to the American people why, in the face of the steady reports of Chinese cyber spying, the concern is misplaced. But it cannot simply refrain from making the judgment and sharing it with the public.

—John J. Tkacik, Jr., is Senior Research Fellow in the Asian Studies Center at The Heritage Foundation.

12. Hearing of the House Armed Services Committee on "Recent Security Developments In China"; witnesses: Richard P. Lawless, Deputy Undersecretary of Defense For Asia-Pacific Affairs, and Major General Philip M. Breedlove, Vice Director For Strategic Plans and Policy, Joint Chiefs Of Staff; June 13, 2007. Transcript provided by Federal News Service.
13. Hearing of the House Armed Services Committee on "Recent Security Developments in China," June 13, 2007, transcript prepared by Federal News Service.
14. USCC Testimony, March 29, 2007, p. 7